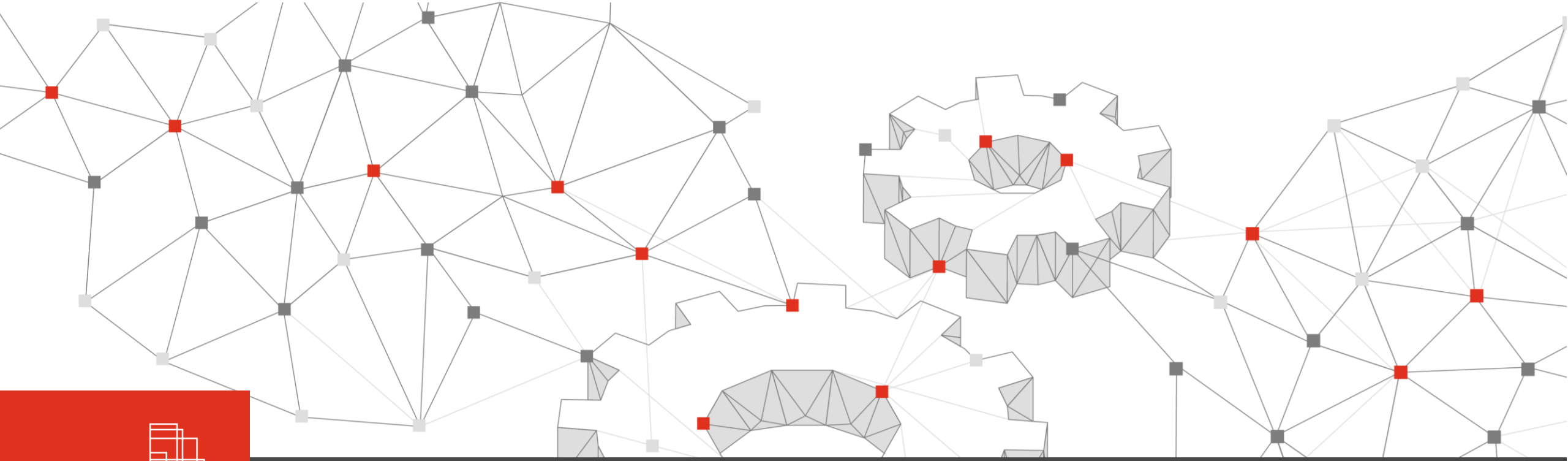
COVID-19

¿Cómo impacta en el ámbito de protección de datos?



Las empresas deben entender el nuevo paradigma de tratamiento de datos personales ante la actual situación de emergencia (1/2)

Principales implicaciones en el ámbito de la Regulación Digital (1/2)

Protección de datos personales

Derecho a la intimidad

Geolocalización

Ciberseguridad

Protección de los datos personales:

- En situaciones de emergencia sanitaria de alcance general, la protección de datos no debería utilizarse para obstaculizar o limitar las medidas que adopten las autoridades públicas, y en concreto las sanitarias
- El Reglamento General de Protección de Datos (en adelante, "RGPD") recoge que debe entenderse lícito el tratamiento de datos personales cuando sea necesario para proteger un interés esencial
- Los datos personales podrán ser tratados sin el consentimiento de los interesados, ya que su tratamiento puede ampararse en las excepciones recogidas en el RGPD:
  - Para cumplir con las obligaciones en el ámbito del Derecho laboral y de la seguridad y protección social
  - Para proteger el interés vital del interesado o de otra persona
  - Por razones de un interés público esencial
  - Para realizar diagnósticos medicos
  - Por razones de interés público en el ámbito de la salud pública

Derecho a la intimidad y uso de dispositivos personales en el ámbito laboral:

- Las iniciativas de teletrabajo deben adoptarse con las debidas garantías de confidencialidad y seguridad de los sistemas
- A nivel organizativo, se deben articular los correspondientes protocolos para un adecuado control y monitorización, y se deben adaptar las fórmulas de medición del desempeño y de cumplimiento de la jornada laboral
- Es necesario Establecer pautas de actuación cuando se permita trabajar desde dispositivos personales (BYOD), previendo incidencias y situaciones de mayor exposición de la información confidencial de la compañía
- El acceso de la compañía a contenidos de los medios digitales facilitados se debe limitar al control del cumplimiento de las obligaciones laborales o estatutarias
- La entidad pertinente deberá aplicar las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado garantizando la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas

Las empresas deben entender el nuevo paradigma de tratamiento de datos personales ante la actual situación de emergencia (2/2)

Principales implicaciones en el ámbito de la Regulación Digital (2/2)

Protección de datos personales

Derecho a la intimidad

Geolocalización

Ciberseguridad

Geolocalización de los ciudadanos por parte del Estado:

- Con carácter especial, y "con el fin de controlar las enfermedades transmisibles, la autoridad sanitaria, […], podrá adoptar las medidas oportunas para el control de los enfermos, de las personas que estén o hayan estado en contacto con los mismos y del medio ambiente inmediato, así como las que se consideren necesarias en caso de riesgo de carácter transmisible" (Ley Orgánica 3/1986, modificada mediante Real Decreto-ley 6/2020, de 10 de marzo)
- A pesar de que la legislación europea impide aplicar estas medidas de vigilancia de la población, el estado de alarma decretado en algunos países podría empujar a los gobiernos a emplear la tecnología de 'Big Data' para evitar la propagación. El mecanismo utilizado podría consistir en una aplicación móvil que los ciudadanos instalarían en sus smartphones a través de la cual el Estado podría geolocalizar a aquellas personas infectadas o con riesgo de ser infectadas

Ciberseguridad en el teletrabajo:

- Los ciberdelincuentes aprovechan situaciones de miedo y alarma colectiva para sacar provecho
- Tratarán de suplantar organizaciones legítimas con información relevante sobre el COVID-19 simulando prestar ayuda, acompañamiento y consejo: en la mayoría de los casos se solicitará que se abra un archivo o que se acceda a un enlace de internet para obtener información del usuario
- Es necesario seguir las recomendaciones facilitadas por la AEPD (Agencia Española de Protección de Datos), que reproducimos a continuación:
  - Mantenerse informado mediante fuentes oficiales y confiables, acudiendo directamente a las webs de las instituciones
  - Verificar la dirección de correo electrónico remitente del mensaje
  - Evitar facilitar datos personales a través de webs a las que se ha accedido siguiendo un enlace contenido en un mensaje o correo electrónico
  - Desconfiar de mensajes con faltas ortográficas, errores gramaticales, saludos genéricos o solicitudes con urgencias injustificadas

Más información

Puede ampliar información a través de su contacto habitual en PwC o a través de nuestros especialistas:

Assumpta Zorraquino
assumpta.zorraquino@pwc.com

Fernando Fernández-Miranda
fernando.fernandez-miranda.vidal@pwc.com

Alejandra Matas
alejandra.matas.brancos@pwc.com

pwc.com/es